WHAT IS CLAIMED IS:

1. A system for binding copy protection to a device comprising:

a key derived in part from at least one preselected unique or distinctive hardware, software or firmware identifier within the device and in part from a random or pseudo-random number; and

a copy protection program securely holding protected content which validates the device based upon the key when employed to access the protected content.

2. The system as set forth in Claim 1 wherein the copy protection program validates the device by:

accessing a value within the device for the at least one preselected hardware, software or firmware identifier;

retrieving a stored value relating to the key from a storage location within the device;

computing a value for the key from the accessed value for the at least one preselected hardware, software or firmware identifier and the stored value relating to the key; and

at least one of:

controlling access to the protected content based upon a comparison of the computed value for the key and the stored value relating to the key; and

employing the computed value for the key to decrypt the protected content.

3. The system as set forth in Claim 2 wherein the key is derived in part from a plurality of preselected unique or distinctive identifiers for hardware, software or firmware within the device.

4. The system as set forth in Claim 2 wherein the key is employed to control access to the protected content without being employed to encrypt or decrypt the protected content, thereby allowing the protected content to be copied or transferred from the device to another device.

5. The system as set forth in Claim 2 wherein the stored value relating to the key contains only the random or pseudo-random number.

6. A device for storing or playing protected content comprising:

at least one hardware, software or firmware component within the device having associated therewith a unique or distinctive identifier; and

a copy protection program selectively executable within the device and securely holding the protected content, wherein the copy protection program, when employed to access the protected content, validates the device based upon a key derived in part from the identifier for the at least one hardware, software or firmware component and in part from a random or pseudo-random number.

7. The device as set forth in Claim 6 wherein the copy protection program validates the device by:

accessing a value within the at least one hardware, software or firmware component for the associated identifier;

retrieving a stored value relating to the key from a storage location within the device;

computing a value for the key from the accessed value for the identifier associated with the at least one hardware, software or firmware component and the stored value relating to the key; and

at least one of:

controlling access to the protected content based upon a comparison of the computed value for the key and the stored value relating to the key; and

employing the computed value for the key to decrypt the protected content.

8. The device as set forth in Claim 7 wherein the key is derived in part from each of a plurality of unique or distinctive identifiers for preselected hardware, software or firmware components within the device.

9. The device as set forth in Claim 7 wherein the key is employed to control access to the protected content without being employed to encrypt or decrypt the protected content, thereby allowing the protected content to be copied or transferred from the device to another device.

10. The device as set forth in Claim 7 wherein the stored value relating to the key contains only the random or pseudo-random number.

11. A method for storing or playing protected content within a device having at least one hardware, software or firmware component with a unique or distinctive identifier associated therewith comprising:

executing a copy protection program within the device which securely holds the protected content, wherein the copy protection program, when employed to access the protected content, validates the device based upon a key derived in part from the identifier for the at least one hardware, software or firmware component and in part from a random or pseudo-random number.

12. The method as set forth in Claim 11 wherein the copy protection program validates the device by:

accessing a value within the at least one hardware, software or firmware component for the associated identifier;

retrieving a stored value relating to the key from a storage location within the device;

computing a value for the key from the accessed value for the identifier associated with the at least one hardware, software or firmware component and the stored value relating to the key; and

at least one of:

controlling access to the protected content based upon a comparison of the computed value for the key and the stored value relating to the key; and

employing the computed value for the key to decrypt the protected content.

13. The method as set forth in Claim 12 wherein the step of computing a value for the key from the accessed value for the identifier associated with the at least one hardware, software or firmware component and the stored value relating to the key further comprises:

deriving the key in part from each of a plurality of unique or distinctive identifiers for preselected hardware, software or firmware components within the device.

14. The method as set forth in Claim 12 wherein the step of controlling access to the protected content based upon a comparison of the computed value for the key and the stored value relating to the key further comprises:

employing the key to control access to the protected content without employing the key to encrypt or decrypt the protected content, thereby allowing the protected content to be copied or transferred from the device to another device.

15. The method as set forth in Claim 12 further comprising:

storing only the random or pseudo-random number within the storage location within the device.

16. A software key for binding copy protection to a device and transmitted within a signal to the device comprising:

a first portion derived from at least one preselected unique or distinctive hardware, software or firmware identifier within the device; and

a second portion derived from a random or pseudo-random number,

wherein the key is employed by a copy protection program securely holding protected content within the device to validate the device when employed to access the protected content.

17. The software key as set forth in Claim 16 wherein the first portion is derived from each a plurality of preselected unique or distinctive identifiers for hardware, software or firmware within the device.

18. The software key as set forth in Claim 16 wherein the key is employed by the copy protection program to control access to the protected content without being employed to encrypt or decrypt the protected content, thereby allowing the protected content to be copied or transferred from the device to another device.

19. The software key as set forth in Claim 16 wherein only the random or pseudo-random number is stored within the device.

20. The software key as set forth in Claim 16 wherein only the random or pseudo-random number is transmitted within the signal to the device.